UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BRADLEY COOPER, on behalf of himself and all others similarly situated,

Plaintiff,

v.

BONOBOS, INC.,

Defendant.

Case No. 1:21-cv-854-JMF

DEFENDANT'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION TO DISMISS THE AMENDED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Other Authorities

Plaintiff Bradley Cooper's ("Cooper") Amended Class Action Complaint (the "Amended Complaint"), ECF No. 28, fails to rehabilitate the deficiencies in his original complaint. Outside of attempting to manufacture injury through the purchase of credit services and a subscription to a spam blocking application, and generic allegations of an increase in spam—both insufficient to confer standing—the Amended Complaint adds no factual allegations of any actual or imminent injury as a result of the security incident suffered by Bonobos. Instead, the Amended Complaint is premised on flawed theories of injury—namely, a speculative risk of identity theft, time and costs expended on that speculative risk, and a vague assertion of unquantified loss of value of his personal information. The law does not permit such claims.

As the Second Circuit recently clarified, a data security incident does not automatically result in cognizable injury to those whose information may be affected, and allegations of an increased risk of future harm can only be considered an injury where the risk is sufficiently "concrete, particularized, and . . . imminent" to qualify as a cognizable injury. *McMorris v. Carlos Lopez & Assocs.*, No. 19-4310, 2021 WL 1603808, at *4 (2d Cir. Apr. 26, 2021) (citation omitted). Here, Cooper devotes several pages of the Amended Complaint to articles about identity theft and various risks when certain kinds of information are stolen, but he fails to plead facts suggesting that he or any of the other individuals whose data was impacted has been or will be the victim of identity theft as a result of the security incident. Nor could he. The data elements involved here are not "immutable" and cannot be "wielded to identify [the victims] and target [them] in fraudulent schemes and identify theft attacks." *McFarlane v. Altice USA, Inc.*, No. 20-CV-1297 (JMF), 2021 WL 860584, at *4 (S.D.N.Y. Mar. 8, 2021) (Furman, J.) (citation omitted). To the contrary, they are the type of information that courts, including the Second Circuit, have found not sensitive and not likely to create a high risk of future harm. Therefore, any generalized fear of

speculative future injury, and time and costs spent monitoring accounts, cannot manufacture injury sufficient to confer standing. Without factual allegations supporting an injury-in-fact that is fairly traceable to the actions of Bonobos, Cooper's claims should be dismissed.

Cooper also fails to allege plausible causes of action. Each of Cooper's claims requires that he suffered some kind of *actual* harm. Cooper has not met this bar. His negligence claim fails for the additional reason that he has failed to plausibly allege a breach of any duty. Cooper's failure to plead any actual harm or materially misleading conduct by Bonobos likewise dooms his claim under New York General Business Law ("GBL") Section 349. And his unjust enrichment claim fares no better, since he has not pled any enrichment by Bonobos at his expense, any actual loss, or any unjust retention of enrichment that would warrant restitution; and, at any rate, the unjust enrichment claim is improperly duplicative of his negligence and GBL claims, which independently warrants dismissal of the unjust enrichment claim.

At bottom, Cooper seeks to maintain this suit without any actual, cognizable injury. The Amended Complaint should be dismissed under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) for failure to allege an actual injury, let alone one plausibly caused by this security incident, and failure to plead the facts necessary to support his claims.

BACKGROUND

Bonobos owns and operates a men's clothing store chain as a digital storefront and at over 60 physical locations. Am. Compl. ¶ 17. To make a purchase on Bonobos's website, customers create an account, providing basic contact information and their credit card information. *Id.* ¶ 18.

In January 2021, a threat actor called ShinyHunters posted on a hacker forum a Bonobos backup database (the "Security Incident"). *Id.* ¶ 1. Bonobos informed customers via email that an unauthorized third party may have been able to view certain customers' "contact information and encrypted passwords." *Id.* ¶ 4. Cooper received Bonobos's email. *Id.* ¶ 11. Fortunately,

encryption protected customers' account passwords. *Id.* ¶¶ 3-4. Bonobos also took the additional precautionary step of disabling the then-current passwords for the potentially affected customers and required them to create new passwords. *Id.*

On January 29, 2021, Cooper and Darrell Kemp filed this putative class action. After Bonobos moved to dismiss and moved to compel arbitration as to Plaintiff Kemp, Cooper filed the Amended Complaint, which, among other things, dropped Kemp as a named plaintiff. Although inconsistently, Cooper alleges at different places in the Amended Complaint that email addresses, phone numbers, the last four digits of credit card account numbers, account order information, encrypted passwords, password histories, customer email addresses, and customer internet protocol ("IP") addresses were impacted in the Security Incident. *See e.g., id.* ¶ 1, 3. The Amended Complaint does not allege that Social Security numbers ("SSNs") were impacted in the Security Incident, nor does it allege that Bonobos collects this type of data. The Amended Complaint also does not allege that dates of birth, drivers' license numbers or other government issued numbers, full credit card numbers, or passwords in plain text were impacted in the Security Incident.

As to the impact of the Security Incident, Cooper alleges that he "began receiving a material increase in suspicious text messages and emails," but includes no allegations as to the content of these messages, when after the Security Incident the alleged increase occurred, or why any alleged "material increase" in "suspicious" messages (which were already occurring prior to this incident) is related to the Security Incident. *Id.* ¶ 11. Cooper also alleges that he bought a subscription to a spam text and phone call blocking application and—although neither his full credit card number nor his SSN was impacted—he put a security freeze on his credit and purchased credit services. *Id.* ¶ 11.

Besides identifying the above, Cooper alleges that he has suffered "one or more" of a host of unspecified injuries, such as (1) a speculative risk from future identity theft and "potential fraud"; (2) the diminishment in value of his personal information; and (3) time and money spent to monitor and prevent against a risk of future identity theft. But Cooper does not identify which injuries, out of this laundry list, he himself has suffered. *Id.* ¶¶ 14, 66. Nor does Cooper allege that he or anyone else impacted has suffered any actual or attempted identity theft or other fraudulent activity resulting from the incident.

ARGUMENT

I. The Amended Complaint Should Be Dismissed Pursuant to Rule 12(b)(1) Because Cooper Lacks Article III Standing

Cooper's Amended Complaint should be dismissed under Federal Rule of Civil Procedure 12(b)(1) for lack of subject-matter jurisdiction. Cooper cannot show: "(1) that he . . . suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief." *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020). Cooper has not alleged that he has suffered or will imminently suffer any injury-in-fact, let alone that any such injury was caused by Bonobos.

Allegations of future injury can constitute injury under Article III "if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (internal quotation marks omitted). The mere exposure of the data elements at issue here does not create a concrete *or* imminent injury as a matter of law. *McMorris*, 2021 WL 1603808, at *5 (holding that, when "confronted with allegations that plaintiffs are at an increased risk of identity theft or fraud based on an unauthorized data disclosure," a court should consider, among other things, "whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud"). Moreover, Cooper

does not allege sufficient facts explaining how his personal information has lost any value. And he cannot otherwise manufacture standing by spending time and money on credit and spam prevention services to prevent a speculative, implausible risk of identity theft or fraud.

A. The Alleged Personal Information Taken in the Security Incident Is Not Sufficient to Show a Concrete or Imminent Injury

i. Cooper Fails to Allege He Has Suffered Any Actual Injury

Cooper has failed to plead *any* actual injury as a result of the theft or alleged "unauthorized use" of his data. Am. Compl. ¶ 66(a), (b) and (c). The Amended Complaint contains no allegations frequently found in security incident cases to constitute injury-in-fact. Specifically, Cooper does not allege that: (1) he has suffered from any kind of identity theft; (2) fraudulent charges have been made on his credit card(s), bank account(s), or other financial account(s); (3) fraudulent tax returns were filed in his name; or (4) there has been any unauthorized access of any of his digital accounts. In *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017), and *Pena v. Brit. Airways, PLC (UK)*, No. 18-cv-6278 (LDH) (RML), 2020 WL 3989055, at *2 (E.D.N.Y. Mar. 30, 2020)—two data security incident cases in this Circuit that were dismissed for lack of standing—plaintiffs at least alleged that their credit card numbers had been *used*. *See also Steven v. Carlos Lopez and Assocs.*, 422 F. Supp. 3d 801, 804 (S.D.N.Y. 2019) (Furman, J.) (contrasting cases involving fraudulent use of credit cards with mere exposure of the data), *aff'd sub nom McMorris v. Carlos Lopez & Assocs.*, No. 19-4310, 2021 WL 1603808, (2d Cir. Apr. 26, 2021). By contrast, Cooper does not even allege that his credit card numbers have been used.

Instead, Cooper alleges "on information and belief," that the threat actor has engaged in "credential stuffing" with encrypted passwords that it allegedly "cracked."[1] Am. Compl. ¶ 2. As

[1] Cooper also discusses (Am. Compl. ¶¶ 48-54) the alleged threat of "SIM swapping," but includes no allegations that the threat actor here had engaged in SIM swapping or that he has been subject to SIM swapping. The alleged future threat of SIM swapping is addressed *infra* at 12-13.

an initial matter, Bonobos has located no case holding that credential stuffing, even if plausible despite encryption, creates an "actual" injury-in-fact sufficient to confer standing. Setting this aside, Cooper alleges no facts—even after amending his complaint—to support an allegation that he *himself* has suffered from credential stuffing, facts that he would have at his disposal. Namely, Cooper does not allege that he used his "cracked" stolen password as passwords for any account outside of his Bonobos account, thereby making those accounts susceptible to "credential stuffing." *See* Am. Compl. ¶ 36 (stating "[*p*]*eople* typically use the same passwords across all of their websites" but making no allegations about Cooper's password use (emphasis added)). Nor does he make allegations that any of his other accounts have been compromised, much less that those accounts used the same password as his Bonobos account. Cooper's vague allegations of "credential stuffing" are therefore insufficient. *See, e.g.*, *Shetiwy v. Midland Credit Mgmt.*, 15 F. Supp. 3d 437, 447 (S.D.N.Y. 2014) (holding articles pasted in a complaint describing "debt collection practices that could constitute violations of the FDCPA" were insufficient for standing because plaintiffs "failed to plead that such tactics were used *against them*" (emphasis original)).

The alleged uptick in suspicious calls and text messages Cooper allegedly received, Am. Compl. ¶ 11, is likewise not an actual injury. In *Allison v. Aetna, Inc.* for example, faced with allegations that plaintiffs were targeted by phishing emails, the court held that plaintiffs failed to demonstrate any actual injury because (1) they had already identified the emails as phishing emails, thus eliminating any risk of harm, and (2) the phishing emails themselves were evidence that no identity theft had occurred because threat actors would not need phishing emails "if they had already obtained the same [personal information] through unlawful means." No. CIV.A. 09-2560, 2010 WL 3719243, *5 (E.D. Pa. Mar. 9, 2010). Courts in this District have likewise rejected an uptick in unwanted emails and phone calls, even malicious ones, as a sufficient injury for Article

III standing purposes. In *Cherny v. Emigrant Bank*, the court found no injury from spam emails where plaintiff alleged that he used a unique email for his account with the defendant and started receiving spam emails on that account shortly after the email address was allegedly compromised. 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) (citing cases); *see also Bell v. Acxiom Corp.*, No. 4:06CV00485-WRW, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) ("[S]everal courts have held that the receipt of unsolicited and unwanted mail does not constitute actual harm."); *Smith v. Chase Manhattan Bank, USA, N.A.*, 741 N.Y.S.2d 100, 102 (App. Div., 2d Dep't 2002) (holding that an increase in unwanted phone calls is insufficient for injury). Here, Cooper concedes he was receiving spam prior to the incident and that he recognized the messages as spam. As such, he has suffered no injury.

Beyond the above, Cooper also alleges that he has suffered from "one or more of the following" injuries, but that statement is a textbook example of allegations that lack specificity and any indication of actual, concrete injury. Am. Compl. ¶ 66. "It is well established that [a court] need not credit a complaint's conclusory statements without reference to its factual context." *Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 146-47 (2d Cir. 2011) (internal quotation and citation omitted). Courts hold that resort to such "including, but not limited to" language is evidence in and of itself of the insufficiency of injuries. *See Johnson v. LVNV Funding*, No. 13-C-1191, 2014 WL 4852027, at *8 (E.D. Wis. Sept. 29, 2014) (finding as conclusory plaintiff's allegation that he had suffered injuries "including, but not limited to" a bullet point of harms); *Henderson v. Sun Pharm. Indus., Ltd.*, No. 4:11-CV-0060-HLM, 2011 WL 4024656, at *8 (N.D. Ga. June 9, 2011) (dismissing claims for failure to plead injury where plaintiff listed all injuries as "including, but not limited to"). Within this laundry list of injuries he cites, Cooper fails to allege which, if any, he *himself* (as opposed to absent class members) has actually suffered. Further,

although he may not rely on injuries to absent class members to support his own standing, he even fails to cite actual injuries of any person, putative absent class member or otherwise. *See Ross v. AXA Equitable Life Ins. Co*., 115 F. Supp. 3d 424, 432 (S.D.N.Y. 2015) (Furman, J.) (citing *Lewis v. Casey*, 518 U.S. 343, 357 (1996)). This Court should not look to conclusory allegations to support the constitutional standing requirement. *Pedroza v. Ralph Lauren Corp.*, No. 19-cv-08639 (ER), 2020 WL 4273988, at *2 (S.D.N.Y. July 24, 2020) (holding a court need not draw inferences in plaintiff's favor from conclusory allegations).

ii. Cooper Fails to Sufficiently Allege that There is a Risk of Imminent Injury

Faced with no actual injury, Cooper suggests that he faces an imminent risk of harm of identity theft or fraud from the Security Incident. This too fails. When relying on a theory of imminent injury, "allegations of possible future injury are not sufficient" and a "theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409-10 (2013). Such is the case here given the non-sensitive data elements allegedly exposed.

In evaluating whether the risk of injury is imminent or impending under Article III, the Second Circuit recently confirmed that courts in data security matters should consider, among other things, "(1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." *McMorris*, 2021 WL 1603808, *5. Here, as discussed *supra*, there are no allegations of misuse of Cooper's information (or the information of anyone else), thus the second factor outlined by the Court is not met. And the third consideration—the type of data involved—dooms Cooper's claims:

the data allegedly exposed here "reveals that plaintiffs are *not* substantially at risk of identity theft as a result of the exposure." *Id.* at *6 & n.6; *see also Whalen*, 689 F. App'x at 96-97 (contrasting plaintiff's stolen full credit card account number with the theft of SSNs); *McFarlane*, 2021 WL 860584, at *4 (same); *In re Uber Techs., Inc., Data Sec. Breach Litig.*, No. CV 18-2970 PSG (GJSx), 2019 WL 6522843, at *4-5 (C.D. Cal. Aug. 19, 2019). While the "dissemination of high-risk information such as SSNs and dates of birth … makes it more likely that those victims will be subject to future identity theft or fraud," the disclosure of other types of less-sensitive (and often public) information does not pose the same amount of risk. *McMorris*, 2021 WL 1603808, at *5. Based on the data elements allegedly impacted here—email address, telephone number, last four digits of a credit card number, encrypted passwords or password histories, and IP addresses—Cooper cannot plead imminent injury sufficient to meet constitutional standing requirements.

First, Courts in this Circuit have held that the alleged future harm from the disclosure of *full* credit card numbers (much less the last four digits) does not satisfy Article III. For example, in *Whalen*, the Second Circuit held that the theft of plaintiff's full credit card number did not confer standing because the plaintiff "d[id] not allege how she can plausibly face a threat of future fraud" from that theft. 689 F. App'x at 90. Likewise, the Eastern District of New York recently dismissed a complaint where full credit card numbers were exposed because "the threat of future identity theft [was] neither imminent nor plausible . . . no personal information apart from Plaintiff's billing address, such as his date of birth or SSN, was compromised in the breach, which might have allowed for the inference of a likelihood of future identity theft." *Pena*, 2020 WL 3989055, at *2; *see also Katz v. Donna Karan Co., L.L.C.*, 872 F.3d 114, 118-21 (2d Cir. 2017) (dismissing a complaint for FACTA violations for lack of standing based on a store printing ten out of the twelve digits of the plaintiff's credit card number on a receipt—the first six and last four digits). Here,

the Security Incident did not impact full credit card numbers, and Cooper fails to explain how the last four digits might plausibly create imminent harm when controlling precedent has held that the full numbers do not.

Indeed, the impermanence of credit card numbers fatally undercuts Cooper's reliance on that data element. In *McFarlane*, for example, this Court distinguished the theft of SSNs from the theft of full credit card account numbers because of the immutable quality of SSNs: "Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, '[a SSN] derives its value in that it is immutable,' and when it is stolen it can 'forever be wielded to identify [the victim] and target him in fraudulent schemes and identity theft attacks.'" 2021 WL 860584, at *4. Cooper does not allege that his SSN was impacted (nor could he plausibly, because Bonobos does not collect SSNs). Cooper's allegations of the exposure of the last four digits of his credit card number—information contained on any printed receipt—is insufficient for standing.

Second, exposure of basic contact information, as alleged here, is insufficient to create Article III standing too. After all, as the Second Circuit has noted, the basic contact information impacted here (name, address, telephone number, and email address) are not the kinds of information that create a serious risk of harm. *McMorris*, 2021 WL 1603808, at *5 ("By contrast, less sensitive data, such as basic publicly available information, or data that can be rendered useless to cybercriminal does not pose the same risk of future identity theft or fraud to plaintiffs if exposed."); *see also Jackson v. Loews Hotels, Inc.*, No. ED CV 18-827-DMG (JCx), 2019 WL 6721637, * 3 (C.D. Cal. July 24, 2019) (holding that exposure of plaintiff's "name, email address, phone number, and mailing address" did not state a cognizable injury because those are not the "certain types of sensitive information" which had led courts to find an imminent risk of harm); *Provost v. Aptos, Inc.*, No. 1:17-CV-02120-ELR, 2018 WL 1465766, *5 (N.D. Ga. Mar. 12, 2018)

(same for exposure of name, email address, and telephone number); *B.J.F. v. PNI Digital Media Inc*, No. C15-1643-MJP, 2016 WL 4014113, at *2 (W.D. Wash. July 27, 2016) (same for telephone numbers, email addresses, hashed passwords, and credit card information). In the only case Bonobos could locate that considered the risk of exposed IP addresses, a court determined that IP addresses fit into the same category of data that does *not* give rise to an imminent risk of harm. *In re VTech Data Breach Litig.*, No. 15 CV 10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017). And Cooper has not alleged how his IP address could be used to create future harm either.

The basic contact information allegedly disclosed here—name, address, email address, and phone number—are the same types of information publicly available online and are not the types that create a risk of harm. *See* Am. Compl. ¶¶ 1, 26. Indeed, Cooper himself makes this same type of information public. On his public website, he lists his name, email address, and phone number. *See* http://rcc-ventures.com/team/.[2] Cooper likewise included a home address in the original complaint, which was filed unsealed. ECF No. 1, ¶ 16. When a plaintiff's allegedly stolen information is already publicly available, there is no imminent risk of harm from that same data's exposure in a security incident. *See McMorris*, 2021 WL 1603808, at *5; *Fus v. CafePress*, Inc., No. 19-CV-06601, 2020 WL 7027653, *3 (N.D. Ill. Nov. 30, 2020); *Allison*, 2010 WL 3719243, *5. Bonobos is aware of no case which has found standing based on the exposure of such limited contact information, and this Court should decline the invitation to be the first.

[2] The court may consider facts outside of a complaint on a motion to dismiss under Rule 12(b)(1). *Libertarian Party of Erie Cnty. v. Cuomo*, 970 F.3d 106, 120–21 (2d Cir. 2020) (explaining that, when considering a motion to dismiss "for lack of statutory or constitutional power to adjudicate the action," a court may refer to evidence outside the pleadings), *petition for cert. filed*, No. 20-1151 (Feb. 23, 2021).

Third, the exposure of encrypted passwords or password histories is insufficient to confer standing. And Cooper does not allege that his plain text passwords, whether current or historical, were exposed. At least one court considering the exposure of encrypted passwords found that even publicly listed, encrypted passwords do not amount to actual harm. *See In re LinkedIn User Priv. Litig.*, 932 F. Supp. 2d 1089, 1094-95 (N.D. Cal. 2013) (holding plaintiff failed to allege sufficient injury from threat actors putting her encrypted password on a public website because she failed to allege how exposure of an encrypted password was tantamount to identity theft).

And Cooper's allegations of "credential stuffing" and "SIM swapping"[3] as the basis for some future harm requires "the same attenuated chain of possibilities rejected by the [Supreme] Court in *Clapper*." *Steven*, 422 F. Supp. 3d at 806 (internal quotations and modifications omitted). First, the Court must assume that the thieves here *cracked* the encrypted passwords, then "targeted" Cooper based on those cracked passwords. *Id.* In other words, the thieves must "select, from thousands of others, the personal information of [Cooper] and attempt successfully" to credential stuff, obtain information that can be used to steal his identity, and then "steal [his] identit[y]." *Id.*; *see also In re VTech Data Breach Litig.*, 2017 WL 2880102, at *4 ("Perhaps plaintiffs used the same username and password for all of their online accounts, and knowledge of their VTech account credentials gave the hacker access to their PayPal accounts. This is speculation, and plaintiffs do not make such allegations."). And again, Cooper does not allege that he used the same passwords for any other accounts, information he has in his possession.

Likewise, in order to SIM swap, the thieves must, at a minimum, target Cooper and steal his mobile phone number (assuming that Cooper provided Bonobos his mobile phone number at

[3] The primary article Cooper cites for support for his allegations of potential "SIM swapping" is a study involving prepaid phone accounts. Cooper does not allege he himself has a prepaid phone account. *See* https://www.usenix.org/system/files/soups2020-lee.pdf.

all). Then they must learn Cooper's mobile phone carrier, and convince his mobile phone carrier to bypass the carrier's normal authentication procedures, and allow the thieves to swap Cooper's mobile SIM card with their own. Then they must figure out what other online accounts Cooper has, target those other online accounts, and obtain SMS messages from those other online accounts (assuming that those other online accounts utilize SMS messaging to send new passcodes). Only then could the thieves steal whatever Cooper might have in those unknown, other online accounts. The sheer number of intervening steps—each of which on their own requires a number of assumptions—are too many to count. Such theorizing—especially when Cooper has not alleged that he used his Bonobos password for any other accounts—is too speculative and attenuated to pass Article III muster.

Simply put, none of the data elements involved here are enough to show an imminent threat of identity theft sufficient to confer Article III standing.

B. Cooper's Conclusory Allegations of Diminution of Value Do Not Constitute Injury

Similarly, Cooper fails to allege any actual diminution in value or inability to use his alleged personal information. It is not sufficient to make conclusory allegations that a security incident has caused a plaintiff's personal information to lose value: a plaintiff must plead how it has been diminished to constitute injury-in-fact. In the District Court's decision in *Whalen*, for example (which the Second Circuit affirmed), the court made clear that merely alleging consumers place value on keeping their credit card information secure is insufficient for standing purposes because such allegations do not demonstrate "how [plaintiff's] cancelled credit card information lost value." 153 F. Supp. 3d 577, 580-81 (E.D.N.Y. 2015), *aff'd*, 689 F. App'x 89; *see also Pena*, 2020 WL 3989055, at *3 (even assuming plaintiff's credit card information had value, mere allegation that its value had been impaired was insufficient because "Plaintiff has not alleged that

he was offered or forewent any opportunity to profit from the sale of his personal information"); *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016) (no injury-in-fact where plaintiffs had "not alleged that they have attempted to sell their personal information or that, if they have, the [security incident] forced them to accept a decreased price for that information").

Cooper's allegations here fall short of even those found insufficient in *Pena* and *Whalen*, both of which involved *full* credit card account numbers and where the court still found no standing. Cooper makes no allegations explaining how his information specifically has lost value, even after the opportunity to amend his complaint. Instead, he generally concludes that he has been harmed by: (1) "the inability to use [his] Private Information" and (2) the "diminution in value of [his] Private Information," Am. Compl. ¶ 66(b) and (f), and references generic online articles regarding the loss of value of other types of data, like full credit card numbers and plain text passwords. *Id* ¶¶ 35-54. But Cooper's vague allegations fail to state a cognizable Article III injury because he has not pled any facts supporting how the Security Incident has caused any loss of use or "diminution of value" of *his* personal information. *See Amidax Trading Grp.*, 671 F.3d at 146-47 (noting conclusory allegations are insufficient to support standing).

C. Cooper Cannot Manufacture Standing By Taking Steps To Prevent A Wholly Speculative Risk of Injury

Cooper's allegations that he has been harmed by taking steps to ameliorate the Security Incident, including the purchase of a subscription to a spam blocking application and credit services, Am. Compl. ¶¶ 11-12, 28, or that he has suffered "annoyance, interference, and inconvenience," *id.* ¶ 3, likewise fail to state a cognizable injury. Courts, including the Second Circuit, routinely hold that allegations of ameliorative steps taken and corresponding "lost time" are insufficient for Article III standing. In *McMorris*, the Court noted that any theory of injury "by means of the time and money spent monitoring or changing . . . financial information and

accounts . . . would fail for the simple reason that [plaintiff] has failed to show that she is at a substantial risk of future identity theft, so the time [she] spent protecting herself against this speculative threat cannot create an injury." *McMorris*, 2021 WL 1603808, at *6, n. 7 (quoting *In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017)) (internal quotation marks omitted). Similarly, in *Pena*, the court found that "the time and expense Plaintiff allegedly devoted to credit monitoring and the mitigation of the identity theft, are not redressable injuries." 2020 WL 3989055, at *3. And in *Whalen*, the District Court noted that "the Supreme Court has dismissed this type of argument" about lost time and money associated with credit monitoring and other mitigation expenses, because plaintiffs "cannot manufacture standing through credit monitoring." 153 F. Supp. 3d at 581 (internal quotations omitted); *Shafran v. Harley-Davidson, Inc.*, No. 07 Civ. 01365(GBD), 2008 WL 763177, at *3 (S.D.N.Y. Mar. 20, 2008) (costs of monitoring for identity theft and fraud do not confer standing); *Tsao v. Captiva MVP Rest. Partners*, 986 F.3d 1332, 1344-45 (11th Cir. 2021) (plaintiff could not manufacture standing by inflicting injuries on himself based on "insubstantial, non-imminent risk of identity theft").

The only out-of-pocket costs that Cooper alleges with regards to the Security Incident is credit services and the purchase of a subscription to a spam blocking application. Am. Compl. ¶ 11. But as this Court has held, allegations of money spent "monitoring or changing . . . financial information and accounts" following a data security incident do not confer standing because plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Steven*, 422 F. Supp. 3d at 807. Cooper cannot demonstrate actual injury or an imminent threat of injury related to the alleged theft or "unauthorized use" of his personal information, much less one related to the Security Incident, and therefore lacks standing to bring the present action.

D. Cooper Has Failed to Allege That Any of His Supposed Injuries Were Caused by Bonobos

Facing no actual injury or risk of injury, Cooper revised his complaint to allege a "material increase" in unwanted texts and phone calls—which, as discussed *supra* at 6-7, does not constitute injury—but, even if it did, Cooper fails to plausibly allege that these texts and phone calls were "caused by [Bonobos]." *Thole*, 140 S. Ct. at 1618. In the context of a data security incident, a plaintiff must plead a nexus between an alleged harm and the incident "beyond allegations of time and sequence." *Welborn v. IRS*, 218 F. Supp. 3d 64, 79 (D.D.C. 2016).

Cooper does not do so. First, Cooper implicitly concedes that he was receiving these texts and phone calls prior to the Security Incident. As a result, Cooper cannot plausibly allege that the Security Incident caused these spam messages or any increase in them. Second, Cooper fails to allege that his phone numbers were unlisted or that these unwanted calls or texts contained information that was disclosed in the incident. Indeed, the only causation argument Cooper makes is that this "material increase" began "after" the Security Incident. Am. Compl. ¶ 11. But a mere temporal nexus is insufficient for standing, and Cooper "seems to simply be one among the many of us who are interrupted in our daily lives by unsolicited calls." *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 33; *see also Cherny*, 604 F. Supp. 2d at 609; *Bell*, 2006 WL 2850042, at *2; *Smith*, 741 N.Y.S.2d at 102.

At bottom, Cooper cannot demonstrate either an actual or imminent threat of injury related to the alleged theft or "unauthorized use" of his personal information, much less one related to the Security Incident. Because Cooper has pled no injury-in-fact, there can be no causal connection between any non-existent injury and the Security Incident. *See, e.g., SAIC*, 45 F. Supp. 3d at 19-20 (holding plaintiffs failed to plead traceability because an increase in spam could not be traced to the security incident when plaintiffs' contact information was publicly available or was not

alleged to be unlisted). The Amended Complaint should be dismissed for lack of subject-matter jurisdiction.

II. The Amended Complaint Should Be Dismissed Pursuant to Rule 12(b)(6) Because It Fails to State a Claim Upon Which Relief May Be Granted

Separately and independently, the Amended Complaint should be dismissed because it fails to state a cause of action under Federal Rule of Civil Procedure 12(b)(6). While considering a motion to dismiss, a court must "accept as true all factual allegations and draw from them all reasonable inferences," but a court is "not required to credit conclusory allegations or legal conclusions couched as factual allegations." *Dane v. UnitedHealthcare Ins. Co.*, 974 F.3d 183, 188 (2d Cir. 2020) (internal modifications omitted). Cooper's Amended Complaint fails to state any viable claims: (1) his negligence claim fails because he cannot show a breach of any duty by Bonobos or that he suffered any proximately caused, actual damages; (2) his GBL claim lacks allegations of a materially misleading act or omission or any harm from any such act or omission; and (3) restitution under an unjust enrichment claim is improper because he cannot show that Bonobos was enriched at his expense, that he suffered any actual loss that would justify restitution, and, at any rate, this claim is improperly duplicative of his negligence and GBL claims.

A. Cooper Fails to State a Claim for Negligence Because He Cannot Show Any Breach of Duty or Proximately Caused Harm

For the same reason Cooper cannot meet Article III's standing requirement, his negligence claim fails because Cooper does not plead any actual or future harm, a required element under New York law. *Caronia v. Philip Morris USA, Inc.*, 715 F.3d 417, 428 (2d Cir. 2013) (citing *Akins v. Glens Falls City School Dist.*, 424 N.E.2d 531, 535 (NY 1981)). Moreover, Cooper has failed to plead: (1) a breach of any duty and (2) proximate causation of any harm—both required elements of their negligence claim—with anything more than conclusory assertions. *Id.*

First, Cooper fails to plausibly allege a duty as a matter of law. In the Amended Complaint, Cooper added allegations pointing to three distinct sources for duties, but none are sufficient. First, he asserts a common law duty based on an "express undertaking to protect class members' personal information and . . . accepting and storing Plaintiff's and Class members' Private Information." Am. Compl. ¶¶ 78-80. But this assertion does not align with those duties courts in New York (and around the country) have held arise in the context of protecting customer data. *See Abdale v. N. Shore-Long Island Jewish Health Sys., Inc.*, 19 N.Y.S.3d 850, 859-60 (Sup. Ct. 2015) (holding company's privacy policy was not "an unlimited guarantee" that a company's systems storing consumers' data could not be stolen by third-party threat actors); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 476 (D. Md. 2020) (finding no common-law duty to safeguard user's personal information under Illinois law); *Dep't of Labor v. McConnell*, 828 S.E.2d 352, 358 (Ga. 2019) (same under Georgia law). Second, Cooper alleges that he and Bonobos have a "special relationship." Am. Compl. ¶ 86. But he fails to identify what that "special relationship" is and why such a relationship would place duties on Bonobos. *Id.* This may be because the customer-store relationship is not one of the kinds of relationships found to be a "special relationship" warranting protection of a plaintiff's data. *Compare Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 748 (S.D.N.Y. 2017) (finding "special relationship" in employer-employee relationship) *with Andres v. LeRoy Adventures, Inc.*, 607 N.Y.S.2d 261, 262 (App. Div., 1st Dep't 1994) (finding no "special relationship" in customer-restaurant relationship). Third, Cooper alleges that Bonobos owed him "independent duties under state and federal laws" in a wholly conclusory fashion. Am. Compl. ¶ 87. But he does not identify a single state or federal law under which Bonobos owed him a duty, likely because there is none. *Cf.*

Smahaj v. Retrieval-Masters Creditors Bureau, Inc., 131 N.Y.S.3d 817, 824-25 (Sup. Ct. 2020) (rejecting customer's claim that HIPAA supplied statutory duty to safeguard data from hacking).

Second, even assuming a common law duty to safeguard the data at issue, Cooper has failed to adequately plead that Bonobos breached that duty. Cooper alleges in a wholly conclusory fashion that "Defendant improperly and inadequately safeguarded Plaintiff's and Class members' Private Information in deviation of standard industry rules, regulations, and practices," but does not specify what standards or guidelines Bonobos failed to follow. *See* Am. Compl. ¶¶ 34, 63, 84, 90. As courts in this District have held, "formulaic recitation[s]" of a breach of duty, such as "Defendant deliberately and/or recklessly did not maintain reasonable procedures designed to protect against unauthorized access," are insufficient to survive a motion to dismiss. *Willey v. J.P. Morgan Chase, N.A.*, No. 09 Civ. 1397(CM), 2009 WL 1938987, at *4 (S.D.N.Y. July 7, 2009). Indeed, a complaint is deficient if it lacks factual allegations "that describe any insufficiency in [defendant's] security procedures, or . . . allegations that [defendant] lacked such procedures" or an explanation of "how the procedures [defendant] adopted failed to comply with [an industry group's] Guidelines." *Id.*; *see also Dane*, 974 F.3d at 188 (on a motion to dismiss, "threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice"). Just as in *Willey*, Cooper has pled nothing more than a threadbare recitation of the elements of his negligence claim supported by conclusory assertions that Bonobos has not followed industry guidelines and/or breached its duty to Cooper. Indeed, the Amended Complaint makes only fleeting reference to "PCI DSS guidelines" with no explanation of the connection between those standards and the Security Incident or Bonobos's practices. Am. Compl. ¶ 63. Cooper has failed to plead facts that would demonstrate how Bonobos fell short, other than that a

security incident occurred, which amounts essentially to a theory of strict liability. Cooper's negligence claim should be dismissed for failing to adequately plead breach of any applicable duty.

Third, Cooper has failed to plead any actual harm stemming from such a breach. As discussed *supra* at 5-17, Cooper's alleged injuries are all purely speculative and conclusory: Cooper does not allege that he has suffered identify theft or any fraud or that he has personally suffered any losses other than manufactured losses related to the time and money spent monitoring his accounts. This is legally insufficient to maintain a claim. *Shafran*, 2008 WL 763177, at *3 (predicting New York courts will hold that "the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy" for several types of claims, including negligence claims); *see also Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1020-21 (D. Minn. 2006) (holding credit monitoring costs are insufficient to show actual damages that would support a negligence action). Nor is Cooper's claim that he has been injured by the loss of his privacy, Am. Compl. ¶ 66(g), legally cognizable in New York, because New York does not recognize a common-law privacy tort. *Valeriano v. Rome Sentinel Co.*, 842 N.Y.S.2d 805 (App. Div. 4th Dep't 2007) (dismissing negligence claim for loss of privacy because New York does not recognize a common law privacy tort).

Fourth, Cooper's alleged future injuries are insufficient to support a negligence claim. Under New York law, a plaintiff's alleged harm in a negligence action may not be premised on "a chain of gross speculations on future events." *Phillips-Smith Specialty Retail Grp. II, L.P. v. Parker Chapin Flattau & Klimpl, LLP*, 696 N.Y.S.2d 150, 152 (App. Div. 1st Dep't 1999). That is all that Cooper alleges here. All of Cooper's future injuries rely on a speculative and attenuated chain of events: namely, his encrypted passwords getting cracked, use of those passwords for

multiple accounts, credential stuffing attacks succeeding on those other accounts and/or successful SIM swapping, and further data being gained through credential stuffing. *Id.* This is not enough.

Fifth, even if Cooper had alleged a cognizable harm, he has failed to allege how it was proximately caused by the Security Incident. Indeed, because Cooper has failed to plead fairly traceable harm for the purpose of Article III standing, *supra* at 5-17, he necessarily fails to show proximate causation because the "fairly traceable standard is lower than that of proximate cause." *Rothstein v. UBS AG*, 708 F.3d 82, 91-92 (2d Cir. 2013) (internal quotations and citation omitted). Cooper does not plead in anything more than a conclusory fashion that Bonobos's alleged acts were a proximate cause of his alleged injuries, and as discussed *supra*, Cooper concedes that his supposed injuries were occurring prior to the incident. This is insufficient for the higher bar of proximate cause.

Since Cooper fails to plead a breach of any duty in more than conclusory terms and any proximately-caused, cognizable harm, his negligence claim should be dismissed.

B. Cooper Fails to State a Claim for Violation of GBL Section 349 Because He Fails to Sufficiently Allege a Materially Misleading Act or Omission and Resulting Damages

Cooper's claims under GBL Section 349 fail because he does not allege a materially misleading statement or omission by Bonobos or any resulting damages. *Stutman v. Chem. Bank*, 731 N.E.2d 608, 612 (N.Y. 2000). State courts have held that, in the data security context, a promise to protect a plaintiff's privacy does not become materially misleading simply because a data security incident occurs; such promises "do not constitute an unlimited guarantee that [personal] information c[annot] be stolen or that computerized data c[annot] be hacked." *Abdale*, 19 N.Y.S.3d at 859-60 ("Defendants' alleged failure to safeguard plaintiffs' protected [personal] information and identifying information from theft did not mislead the plaintiffs in any material way and does not constitute a deceptive practice within the meaning of [GBL § 349]."). The only

potential misstatements or omissions Cooper points to is Bonobos's privacy policy, which states that "Bonobos has implemented an information security program that includes administrative, technical and physical controls reasonably designed to safeguard your personal information." Am. Compl. ¶ 22 (internal modifications omitted). But Cooper does not allege that Bonobos lacked an information security program with reasonably designed "administrative, technical, and physical controls." And, in any event, that statement, like the statements in *Abdale*, is not misleading.

Moreover, the policy has no material omission, and Cooper points to none. Misleading omissions are actionable under the GBL "where the business alone possesses material information that is relevant to the consumer and fails to provide this information." *In re Sling Media Slingbox Advert. Litig.*, 202 F. Supp. 3d 352, 359 (S.D.N.Y. 2016) (quoting *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank*, 647 N.E.2d 741, 745 (N.Y. 1995)). To plead a viable omission claim under the GBL, a plaintiff must "plausibly allege that the defendants *had knowledge* of the material information and failed to disclose or actively concealed such information." *Id.* (internal quotations and modifications omitted). In other words, "a defendant's failure to reveal facts about which even it was unaware at the time will not lead to liability under § 349." *Id.* Like in *Sling* and *Abdale*, Cooper fails to allege that Bonobos was aware of any security vulnerabilities that it failed to disclose, instead alleging that Bonobos "knew or *should have known*" that its systems were not up to date. Am. Compl. ¶ 98 (emphasis added). But "should have known" is not enough. As such, Cooper has not pled a viable GBL claim based on omissions.

Cooper's GBL claim is also deficient because he fails to plead any actual damages he has suffered from any deceptive practice. *See Mount v. Pulsepoint, Inc.*, No. 13 Civ. 6592 (NRB), 2016 WL 5080131, at *4 (S.D.N.Y. Aug. 17, 2016) (refusing to find harm under GBL where company allegedly took consumer's browser data surreptitiously through tracking cookies); *see*

also Smith, 741 N.Y.S.2d at 102 (holding sale of customers' names, addresses, and financial information to third-parties in violation of customer privacy policy failed to state any damages since plaintiff failed to state any actual loss from sale of names). Cooper cannot show otherwise by alleging he would not have bought products from Bonobos if he knew about Bonobos's security practices. *See Small v. Lorillard Tobacco Co*., 720 N.E.2d 892, 898 (N.Y. 1999). Nor may he save his claim by manufacturing a harm via credit services or subscription to a spam blocking application over unjustified and speculative fears of identity theft. *Shafran*, 2008 WL 763177, at *3 (holding that "the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy" for, among other claims, GBL claims). Since Cooper cannot plead an objectively and materially misleading act or omission, or any subsequent harm, his GBL claim should be dismissed with prejudice.

C. Cooper Fails to State a Claim for Unjust Enrichment Because He Fails to Sufficiently Allege that Any Enrichment Would Warrant Restitution and the Claim Is Duplicative of His Negligence and GBL Claims

Cooper's unjust enrichment claim is also unavailing. Under New York law, "[a]n unjust enrichment claim has three elements: first, the defendant was enriched; second, the enrichment was at the plaintiff's expense; and third, the defendant's retention of the benefit would be unjust." *Mount*, 2016 WL 5080131, at *13. Here, Cooper has failed to plead any of the three elements. And the claim should be dismissed for the additional reason that it improperly duplicates Cooper's negligence and GBL claims, with all three relying on the same factual allegations for support.

Cooper has not sufficiently alleged that Bonobos was enriched at his expense. He does not allege that he failed to receive the value of what he paid for (namely, Bonobos goods). Instead, he suggests that Bonobos profited from the transfer of his information. Am. Compl. ¶ 112-13. But claims that a defendant was enriched at a plaintiff's expense from collecting personal information have not fared well in New York courts. It is not enough to simply claim that a plaintiff would not

have entrusted his information to a retailer absent an obligation to protect a customer's data; such allegations fail to indicate whether the plaintiff paid extra for the security protections beyond the price of the goods or whether proceeds from the purchase of the goods went towards security services. *See Whalen*, 152 F. Supp. 3d at 581. An allegation that Bonobos was enriched because Cooper somehow lost value in his personal information is likewise deficient unless Cooper can also allege that he was unable to continue using the information that was supposedly wrongly retained. *See Edelman v. Starwood Cap. Grp., LLC*, 892 N.Y.S.2d 37, 40 (App. Div. 1st Dep't 2009). Cooper has made none of these allegations, and his unjust enrichment claim fails.

Additionally, as described *supra* at 5-7, Cooper has not alleged that he has suffered any actual loss in conjunction with his purchase, which would be required for restitution. *See Edelman*, 892 N.Y.S. at 40 ("[T]he general rule is that the plaintiff *must have suffered a loss* and an action not based upon loss is not restitutionary." (internal quotations omitted) (emphasis original)). Cooper's allegations of loss from credit services are manufactured from a speculative fear of identity theft, and they cannot sustain this element. *See Shafran*, 2008 WL 763177, at *3.

Moreover, Cooper has failed to meet the last requirement for an unjust enrichment claim—namely, that any benefit retained by the defendant is unjust—because he received what he gave a benefit for in the form of the goods he purchased. *See, e.g., In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, No. 3:12-cv-00325-RCJ-VPC, 2013 WL 4830497, at *4 (D. Nev. Sept. 9, 2013) (no unjust enrichment where plaintiffs "bestowed the benefit of their purchase . . . [and] [d]efendant provided [p]laintiffs a benefit in return (providing the goods)").

Finally, even if Cooper had pled the elements of unjust enrichment, his claim still fails because it is duplicative of his GBL and negligence claims. An unjust enrichment claim is not a "catchall cause of action to be used when others fail": unjust enrichment is not "available where it

simply duplicates, or replaces, a conventional contract or tort claim." *Corsello v. Verizon N.Y., Inc.*, 967 N.E.2d 1177, 1185 (N.Y. 2012). In the wake of *Corsello*, courts in this District have "routinely dismiss[ed]" unjust enrichment claims which rely on the same factual allegations as other claims such as negligence and violations of GBL Section 349. *Twohig v. Shop-Rite Supermarkets, Inc.*, No. 20-CV-763 (CS), 2021 WL 518021, at *9 (S.D.N.Y. Feb. 11, 2021) (dismissing unjust enrichment claim as duplicative of negligence, fraud, and GBL Section 349 claims); *see also, e.g.*, *Barreto v. Westbrae Nat., Inc.*, No. 19-cv-9677 (PKC), 2021 WL 76331, at *8 (S.D.N.Y. Jan. 7, 2021) (same for negligence, fraud, and GBL Section 349 claim); *Alce v. Wise Foods, Inc.*, No. 17 Civ. 2402 (NRB), 2018 WL 1737750, at *11-12 (S.D.N.Y. Mar. 27, 2018) (same for GBL Section 349 claim). Dismissal of duplicative unjust enrichment claims is warranted even if the other claims are dismissed because, while unjust enrichment may be pled in the alternative, such a claim will not survive a motion to dismiss "where plaintiffs fail to explain how their unjust enrichment claim is not merely duplicative of their other causes of action." *Nelson v. MillerCoors, LLC*, 246 F. Supp. 3d 666, 679 (E.D.N.Y. 2017) (dismissing all claims). Here, Cooper's unjust enrichment claim relies on the same factual allegations as his GBL and negligence claims: that Bonobos misrepresented its security policies and therefore that he overpaid Bonobos for goods. *Compare, e.g.,* Am. Compl. ¶ 116 (alleging, in the unjust enrichment count, that Cooper would not have provided his information if he had known of Bonobos's purportedly inadequate security) *with id*. ¶ 100 (alleging the same facts with regards to the GBL count). Since Cooper relies on the same factual allegations to support his unjust enrichment claim, his GBL claim, and his negligence claim, the unjust enrichment claim is duplicative and should be dismissed.

CONCLUSION

For the foregoing reasons, Bonobos respectfully requests that the Court dismiss the Amended Complaint pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6).

Dated: New York, New York
May 5, 2021

Respectfully submitted,

HOGAN LOVELLS US LLP

By: */s/ Michelle Kisloff*

Michelle Kisloff
Allison Holt Ryan (*pro hac vice*)
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
Telephone: (202) 637-5600
michelle.kisloff@hoganlovells.com

Lisa Fried
390 Madison Avenue
New York, NY 10017
Telephone: (212) 918-3000
lisa.fried@hoganlovells.com

Jasmeet K. Ahuja
1735 Market Street, 23rd Floor
Philadelphia, PA 19103
Telephone: (267) 675-4600
jasmeet.ahuja@hoganlovells.com

Counsel for Bonobos, Inc.